





Information Security Program

Rules of Behavior

FOR OFFICIAL USE ONLY

This information is intended for HHS use only.

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Rules of Behavior (RoB) provide general instructions on the appropriate use of Departmental IT resources and apply to all Departmental users, including both civil servants and contractors. All government and contractor staff are required to read this document and sign and submit the accompanying form before accessing Departmental systems and or networks.

The *HHS Rules of Behavior* are not to be used in place of existing policy. Rather, they are intended to supplement the *HHS Information Security Program Policy* and the *HHS Information Security Program Handbook*. Because written guidance cannot cover every contingency, Departmental staff and users are asked to augment these rules and use their best judgment and highest ethical standards to guide their actions. Because these principles are based on federal laws and regulations, and Departmental regulations and directives, there are consequences for failure to comply with the principles of behavior. Violation of these rules may result in suspension of access privileges, written reprimand, suspension from work, demotion, and criminal and civil penalties.

All government and contractor staff must sign this form, acknowledging that they have been made aware of and understand the requirements and responsibilities outlined in this document. Questions about these ROB may be directed to one's supervisor or Contracting Officer's Technical Representative (COTR), or to the Operating Division (OPDIV) Chief Information Security Officer (CISO).

Activities on Departmental network system resources are subject to monitoring, recording, and periodic audits. Authorized IT security personnel may access any "user's" computer system or data communications and disclose information obtained through such auditing to appropriate third parties (e.g., law enforcement personnel). Use of Departmental IT system resources expresses consent by the user to such monitoring, recording, and auditing.

The signed acknowledgement should be submitted to the supervisor or COTR. Each supervisor will be required to file all forms with the OPDIV CISO on an annual basis. On an annual basis, the OPDIV CISOs will be responsible for reporting to the HHS CISO the number of personnel who have been authorized to access Departmental systems and the number and percent of whom have signed the acknowledgement form.

The following pages outline the RoB for several key areas of the Departmental Information Security Program. Please note that these lists are not exhaustive.

E-mail

Government-provided e-mail is intended for official use and authorized purposes. E-mail users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have e-mail privileges withdrawn and may be subject to disciplinary action. Guidance for e-mail use is listed below.

- Limited personal use of Departmental e-mail services is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies.
- Personnel using Departmental e-mail must give consent to having their e-mail monitored. E-mail contents will not be accessed or disclosed other than for security purposes or as required by law.
- Users shall ensure that e-mail communications are free of viruses through regular screening of incoming e-mail traffic and virus-detection updates.
- E-mail spamming (unsolicited commercial e-mail)—sending or forwarding chain letters, other junk e-mail, or inappropriate messages—is not permitted.
- The sending of threatening, obscene, harassing, intimidating, abusive, or offensive material about others is not permitted.
- The use of abusive or objectionable language in either public or private messages is not permitted.
- The sending of messages in support of a “for profit” activity is not permitted.
- The sending of e-mail messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- The transmission of confidential or sensitive information by e-mail, unless protected by Departmental-approved encryption, is not permitted.
- E-mail software should not be left open on computer systems to prevent unauthorized access and misuse.
- Unauthorized Government-wide or agency-wide broadcast messages are not permitted.
- Distribution of unauthorized newsletters is not permitted.

Internet

Government-provided Internet access is intended for official use and authorized purposes. Internet users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have Internet privileges withdrawn and may be subject to disciplinary action. Guidance for Internet use is listed below.

- Limited personal use is acceptable as long as it does not affect the mission of the HHS and does not conflict with laws, regulations, and policies.
- Personnel using Departmental Internet access must give consent to have their actions monitored. Monitoring will not be performed, or its findings disclosed, for reasons other than for security purposes or required by law.
- The act of, or the attempt to, break into another computer (federal or private) or introducing malicious code (e.g., computer viruses, worms, or Trojan horses) is not permitted.
- Certain types of data, such as personal or unauthorized government owned, or non-government owned software is not permitted.
- It is not permitted to send, retrieve, view, display, or print sexually explicit, suggestive text or images, or other offensive material.
- The use of another person's account or identity is not permitted.
- The use of Internet games and chat rooms are not permitted.

Passwords

Passwords are an important aspect of computer security and are the front line of protection for user accounts. Listed below are the password requirements to be used for Departmental information systems.

- Create passwords with a minimum of eight characters.

Use a combination of alpha, numeric, and special characters for passwords, with at least at least one uppercase letter, one lower case letter, and one number.

- Avoid using common words found in a dictionary as a password.
- Avoid obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Change passwords every 90 days.
-
    - The password expiration is a risk based management decision and OPDIVs are encouraged to require a shorter time period for password expiration for more sensitive information.

- Change vendor-supplied passwords immediately.
- Do not reuse passwords.

    - A new password must contain no more than five characters from the previous password.

- Protect passwords by committing them to memory or storing them in a safe place:

    - Do not post passwords.
    - Do not keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.

- Change password immediately if password has been seen, guessed or otherwise compromised.
- Keep user identifications (ID) and passwords confidential.
- Do not accept another user's password, even if offered.
- Report any compromise or suspected compromise of a password.

    - Report incidents to the Secure One Communications Center (SOCC).
    - All parties shall work to preserve evidence of computer crimes in accordance with Departmental guidance.

Equipment

Government-provided equipment is intended for official use and authorized purposes. For the Departmental RoB, there is no distinction between stand-alone and on-line computer systems. Users must exercise common sense, good judgment, and propriety in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have equipment privileges withdrawn and may be subject to disciplinary action. Guidance for equipment use is listed below.

- Using Department-provided equipment is restricted to business purposes.
    - Limited personal use is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies; however, keeping family or personal records, playing computer games, or loading unauthorized software onto government computers is not permitted.
- Personnel using Departmental equipment must give consent to have their actions monitored. Monitoring will not be performed, or its findings disclosed, for reasons other than security purposes or required by law.
- Equipment, software, or computers using locks or an operating system password should not be reconfigured unless operating under Department-approved and applicable standard procedures.
- Protect passwords, information, equipment, systems, and networks to which a user has access.
- Minimize the threat of viruses by write-protecting diskettes, checking "foreign" data for viruses, and never circumventing the anti-virus safeguards of the system.
- Do not leave terminals unattended without password protecting them.
- Report lost or stolen equipment, security incidents, or anything unusual or suspicious immediately to the appropriate OPDIV CISO.

Removal of Equipment

Property passes are to be obtained from the Property Custodial Officer before the removal of any Departmental network equipment from the building.

Software Licensing

Copyright laws and the license agreements accompanying the software on Departmental equipment govern Departmental users' acquisition and use of software. It is the responsibility of all Departmental staff and users to protect Departmental interests in the performance of their duties. This includes responsibility for assuring that commercial software, acquired by Departmental, is used only in accordance with licensing agreements. Likewise, it is also the Department staff and users' responsibility to assure that any proprietary software is properly licensed before being installed on Departmental equipment. Local Area Network (LAN) and personal computer (PC) users are not to download LAN-resident software. All Departmental staff and users should be aware that it is illegal to:

- copy or distribute software or its accompanying documentation, programs, applications, data, codes, and manuals without permission or a license from the copyright owner
- encourage, allow, compel, or pressure, either explicitly or implicitly, operations staff and users to make or distribute unauthorized software copies
- infringe upon the laws against unauthorized software copying because someone requests or compels it
- loan software so that a copy can be made
- make, import, possess, or deal with articles intended to facilitate the removal of any technical means applied to protect the software program.

Furthermore, according to the United States copyright law, persons violating software licensing laws can be subject to civil damages and criminal penalties.

Departmental software rules are as follows:

- Software will not be modified without the approval of both the development team and the Department.
- Software will only be issued, and used by, authorized individuals as prescribed by local authority.
- The addition of personal IT resources to existing Departmental IT resources without written authorization from the OPDIV CISO is not permitted.
- Security features and controls will be activated when processing data.
- Departmental staff and users aware of any misuse of Departmental software shall notify their supervisor, the security manager, or the OPDIV CISO.

Off-Site Computing

Access to Departmental infrastructure via dial-up or broadband connection poses additional security risks, but may be necessary for certain job functions. Since off-site access is allowed, telecommunication logs and Departmental phone records will be reviewed regularly and routine spot checks will be conducted to determine if Departmental business functions are complying with controls placed on the use of off-site access connections. Access to Departmental networks from off-site locations will be monitored by an audit trail security system.

Government-provided off-site access is intended for official use and authorized purposes. Off-site users must exercise common sense and good judgment in the use of government-provided resources. Departmental staff and users who misuse government resources in any way may have off-site access privileges withdrawn and may be subject to disciplinary action. Guidance for off-site access is listed below.

- The Department provides off-site access to personnel for business purposes.
-
    - Limited personal use is acceptable as long as it does not affect the mission of the HHS and does not conflict with laws, regulations, and policies; however, persons other than the authorized HHS user should not be permitted to make use of HHS equipment and/or software.

- Personnel using Departmental off-site access must give consent to having their actions monitored. Monitoring will not be performed or its findings disclosed other than for security purposes or as required by law.
- Departmental staff and users must adhere to the letter and spirit of all applicable federal laws, regulations, contracts, licenses, policies, standards, guidelines, business controls, security rules, and other expectations.
- Departmental staff and users must report lost or stolen equipment, security incidents or anything unusual or suspicious immediately to their appropriate CISO.
- Departmental staff and users must ensure integrity of data created, accessed, or modified.
- Departmental staff and users must provide a secure and protected environment for government data and government-owned computing resources.
- Departmental staff and users must apply required safeguards to protect government/Departmental records from unauthorized disclosure or damage.

Media Control

Departmental staff and users must adhere to Department-wide procedures for access, storage, and transportation of all media containing sensitive information. Procedures include completing logs to track deposits and withdrawals of media from on-site storage facilities, libraries and backup storage facilities, and procedures for the proper wrapping and labeling of media to be mailed or couriered, or the eventual disposal of media.

HHS staff and users who misuse government resources in any way may have media access privileges withdrawn and may be subject to disciplinary action. Guidance for media control is listed below.

- Departmental staff and users should not leave sensitive information, even temporarily, and should monitor it in the following ways:
  - Departmental staff and users must keep sensitive material in a secure safe or locked cabinet and return all sensitive information to the safe at the end of each business day.
  - Departmental staff and users must abide by the physical and environmental protection controls relating to sensitive data that is contained in a media storage vault or library.
  - Departmental staff and users must turn over, place out of sight, or remove from the screen sensitive information when visitors are present.
  - Departmental staff and users must sanitize or destroy diskettes and other magnetic storage media that contain sensitive data when they are no longer needed to store the sensitive data.
  - Departmental staff and users must dispose of both electronic and hard copy media in accordance with Departmental sanitation and disposal policy.

Voice and Data (Fax) Communication

Government-provided voice communication resources are intended for official use and authorized purposes. Departmental staff and users must exercise common sense and good judgment in the use of all voice communication tools. Departmental staff and users who misuse government resources in any way may have privileges withdrawn and may be subject to disciplinary action. Guidance for voice communication is listed below.

- The Department provides voice communication access to personnel for business purposes.
-
  - Limited personal use is acceptable as long as it does not affect the mission of the Department and does not conflict with laws, regulations, and policies.

- Personnel using Departmental voice communication and facsimile resources consent to having their actions monitored. Monitoring will not be performed, or its findings disclosed other than for security purposes or as required by law.
- Attempting to break into another's voice mail (federal or private) is not permitted.
- Sending threatening, obscene, harassing, intimidating, abusive, or offensive material to or about others is not permitted.
- Using abusive or objectionable language in either public or private messages is not permitted.
- Sending messages in support of a "for profit" activity is not permitted.
- Sending or relaying sensitive information over an unencrypted line is not permitted.
- Sending messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- Unauthorized government-wide or agency-wide broadcast messages are not permitted; and distribution of unauthorized messages is not permitted.

Physical Security

Physical access points to sensitive facilities, or restricted areas housing information systems that process or display information are controlled during working hours and guarded or locked during nonworking hours. Access authorization will always be verified before granting physical access and unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Departmental staff and users should wear identification badges at all times.

Departmental staff and users who misuse government resources in any way may have their physical access privileges withdrawn and may be subject to disciplinary action. Guidance for physical security is listed below.

- Only authorized Departmental personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations).
- Departmental users not on the access roster for a limited access room or facility must sign in and be escorted the entire time present in the room or facility.
- All Departmental visitors, contractors, or maintenance personnel must be authenticated through preplanned appointments and ID checks.
- Departmental staff and users should inform physical security officials when a system's sensitivity level requires additional protections and alert physical security leadership to locations that house sensitive equipment.
- Departmental staff and users must report immediately any theft or loss of sensitive equipment to physical security personnel.

Disciplinary Action

The Department has established procedures for disciplinary actions for security violations its staff and users commit. These disciplinary actions may be based on the sensitivity of information involved and the number of prior offenses.

The Department has defined remedial actions for employees to include reassignment of work duties, disqualification from a particular assignment, letter of warning, suspension, and/or termination.

It is expected that Departmental staff and users exercise common sense, good judgment, and propriety in the use of Government-provided resources. Departmental staff and users who misuse government resources in any way may be subject to disciplinary action. Guidance for violation handling is listed below.

- Departmental staff and users must report suspected personnel security violations to the Office of Inspector General (OIG) for investigation and recommended disciplinary action.
- Departmental staff and users are subject to disciplinary actions for security violations specified in security awareness training and the Rules of Behavior.
- The Department may remove contractor staff that commit security violations commensurate with high risk to the Department from the contract, and depending on the security violation, criminal sanctions may also apply.
- Departmental staff and users who purposely disclose their passwords to others to share or transfer access are subject to disciplinary actions.
- Departmental users and staff should be alert to developments, such as a drastic change(s) in work habits, which may increase the potential for security violations, whether intentional or accidental.
- Departmental employees and contractors should be aware that any use of the Internet or e-mail that is illegal, offensive, or in violation of Departmental policies or standards can be the basis for disciplinary action up to and including legal action.
- Departmental staff and users should not allow, encourage, or promote the illegal duplication of software in their possession.
- Departmental staff and users, who purposely make, acquire, or use unauthorized copies of computer software, may be subject to disciplinary action.

Incident Reporting Escalation

The Department has established procedures for incident and violation handling that its staff and users might identify to limit any compromises to the Department. Guidance for incident and violation handling is listed below:

- Departmental users must report any of the following incidents to the Secure One Communications Center (SOCC):
  - malicious code: a virus, worm, Trojan horse, or other code-based entity that is either successful or unsuccessful in infecting a host. This category applies to incidents and events.
  - probes and reconnaissance scans: involve searching the network for critical services or security weaknesses.
  - inappropriate usage: a person violates acceptable computing use policies, such as sending spam, email threats, or making illegal copies of software.
  - unauthorized access: a person gains logical or physical unauthorized access to a network, system, application, data, or other resource. This access may include root compromises, unauthorized data alterations, Web site defacements, loss/theft of equipment, unauthorized use of passwords, and use of packet sniffers.
  - denial of service (DoS) attacks: a successful or unsuccessful attack (including Distributed Denial of Service Attacks) impairs the authorized use of networks, systems, or applications by exhausting resources, to include Distributed DoS attacks.
  - other types of incidents include, but are not limited to:
    - alterations/compromises of information
    - adverse site mission impacts
    - classified system incidents
    - loss or theft of equipment.
- Reporting incidents to the SOCC can be made by phone, email, or through ISDM.
  - E-mail address is: Security.CommunicationsCenter@hhs.gov
  - Phone number is: 202-205-9581
  - ISDM address is: https://intranet.hisp.hhs.gov/hhs/public.
- Departmental users should report these incidents within a 2-hour time frame of the incident occurring.
- All Departmental users and staff should be trained on the appropriate

incident-response handling procedures.

Education and Awareness

The Department has established procedures for ensuring its staff and users receive education and awareness training. Guidance on education and awareness is listed below:

- All Departmental users, including contractors, must receive education and awareness training commensurate with their duties.
- All new Departmental users of IT systems must receive initial training before being authorized network access and within 60 days of appointment.
- All Departmental users must receive annual refresher training.

SIGNATURE PAGE

All government staff and contractors are required to read the Rules of Behavior and are responsible for abiding by its contents. Violations of the Rules of Behavior or computer policies may lead to disciplinary action, up to and including termination of employment. Signing this form acknowledges your understanding of the requirements for access to Departmental IT systems and your responsibilities as a system user.

Signatures:

Employee's/User's Name: _____
(Print)

Organization: _____

Employee's/User's Signature: _____

Date Signed: _____

Supervisor's Name: _____
(Print)

Supervisor's Signature: _____

NOTE: Sign and return this form to your supervisor or COTR. Make a copy for your records and post it in an accessible area. Your supervisor will retain your original, signed acknowledgement form.